HIPAA SECURITY
Compliance Insider
A PLAIN-ENGLISH GUIDE TO HIPAA SECURITY & TCS REGULATIONS

FEBRUARY 2004

IN FUTURE ISSUES

- Use Change Control Form When Adding or Removing Software and Hardware
- How to Create an Effective Password Policy
- Set Policy on UPS Units to Protect EPHI Integrity and Availability

Encryption: What Experts and HIPAA's Security Regs Say You Should Do

If you're like many health care professionals we talked to, you may be confused about whether, and to what extent you should, encrypt your organization's electronic protected health information (EPHI) so that it's difficult for an unauthorized person to decipher. You can encrypt all your EPHI—whether it's in transit, such as an e-mail or file transfer, or at rest, such as information stored on a PC, PDA, or backup tape. But encryption might not always be the best solution to protect your EPHI. Depending on the circumstances, encrypting EPHI can be costly. And it can slow your computer equipment and make communications difficult.

To make matters more confusing, HIPAA's security regulations contain two implementation specifications involving encryption, and they're both addressable. That means you don't have to implement them if you determine that they're not reasonable and appropriate to your organization. But if you don't implement them, the security regulations require you to document your reasons. And you'll still have to implement "equivalent alternative measures" if you can.

To help you decide what you should encrypt, we'll describe what HIPAA's security regulations say about encryption. And we'll tell you what experts around the country recommend when it comes to protecting your EPHI—both when it's at rest and in transit. Plus we'll give you Model Language to include in your security policies if you choose to require encryption of your EPHI.

What the Security Regulations Say

Aside from defining encryption, HIPAA's security regulations mention encryption of EPHI twice—both times in addressable implementation specifications for the technical safeguard standards.

Access control standard. The HIPAA security regulations' access control standard lists "encryption and decryption" as a method for ensuring that only authorized persons have access to EPHI. This standard deals mainly with data at rest, such as EPHI on PCs, PDAs, or backup media. According to HHS, "the use of file encryption is an acceptable method of denying access to information in that file." But the standard *doesn't require* you to encrypt your stored EPHI. In the preamble to the security regulations, HHS explains that "the use of encryption, for the purpose of access control of data at rest, should be based upon an entity's risk analysis."

(continued on p. 2)

Subscriptions: *HIPAA Security Compliance Insider* is published monthly. Subscription rate: $297 for 12 monthly issues. Address all correspondence to: Brownstone Publishers, Inc., 149 Fifth Ave., New York, NY 10010-6801. Tel.: 1-800-643-8095 or (212) 473-8200; fax: (212) 473-8786; e-mail: awatkins@brownstone.com

ENCRYPTION: WHAT YOU SHOULD DO (continued from p. 1)

Transmission security standard. Encryption is also an addressable implementation specification under the security regulations' transmission security standard. That standard requires health care organizations to guard against unauthorized access to EPHI transmitted over an electronic communications network, including the Internet and the organization's internal network. According to the implementation specification, health care organizations must implement a mechanism to encrypt EPHI "whenever deemed appropriate."

So, according to the HIPAA security regulations, whether you should encrypt EPHI at rest or in transit is up to your organization based on the results of your risk analysis. "HIPAA requires health care organizations to manage their EPHI in a way that precludes unauthorized access," says health information technology expert Ann Geyer. Encryption is just one way of doing that, she explains. "If your organization determines that encryption isn't reasonable or appropriate and it can control access in another way, such as restricting EPHI to private networks or using strong authentication methods, it can do that instead," she says.

Consider Encryption in Five Circumstances

Even though the security regulations don't require encryption, the health information security experts we spoke to say there are at least five circumstances in which you should strongly consider encryption.

EPHI transmitted via e-mail and electronic file transfers. Security experts agree that EPHI transmitted via e-mail and the Internet is inherently insecure. If left unprotected, e-mails and files can be opened, forwarded, or tampered with.

"One of the best ways to protect information e-mailed or transferred over the Internet is to encrypt it," says health care security consultant Lesley Berkeyheiser. HHS agrees, encouraging health care organizations, in the preamble to the security regulations, "to consider use of encryption technology for transmitting electronic protected health information, particularly over the Internet." Some providers are choosing to set up an e-mail account and obtain an encryption key that allows them to encrypt their e-mails. "Both the American Medical Association and the California Medical Association will provide public keys for encryption to any licensed physician," says Geyer.

Another common way to encrypt transmitted EPHI is to use a secure Web site, says Geyer. For example, a patient would access his physician's secure Web site over the Internet and send messages to the physician using a Web application on that Web site. When the physician responds to the patient, the Web application e-mails a link that returns the patient to the physician's Web site, where he can retrieve his message. "The Web application takes care of encrypting the messages," says Geyer. One large health plan we spoke to chose this option and forbids e-mailing EPHI.

Here's some Model Language you can include in your security policies if you decide that a secure Web site is also the best choice for you.

Model Language
Employees shall not e-mail patient and customer EPHI using the Internet, a wireless network, or any other public network. All electronic communications containing patient and customer EPHI must be conducted using the Organization's patient or customer Web application established for this purpose.

***Insider* Says:** HHS acknowledges in the preamble to the HIPAA security regulations that small and rural providers may find it difficult to exchange encrypted e-mail with patients. If you choose not to encrypt EPHI in e-mails with patients, make sure your patient acknowledges in writing that e-mail isn't secure and may be intercepted, resulting in a breach of privacy. We'll tell you how, in a future issue.

EPHI transmitted via wireless equipment. EPHI transmitted over wireless equipment always warrants encryption, says health information security expert Jim Klein. "It's not possible to limit access to the medium carrying the signals," he says. Anyone can buy equipment that allows them to "listen" to the wireless network and monitor wireless communications.

Security consultant and author Charles Cresson Wood agrees with this assessment, explaining that "interception of wireless transmissions is quite easy, and many useful details, including user IDs and passwords, can be obtained." Here's Model Language that you can include in your security policies to prevent the wireless transmission of unencrypted EPHI.

Model Language
Wireless technology must never be used for the transmission of unencrypted patient or customer EPHI.

EPHI stored on computer equipment. To prevent the possibility of unauthorized access to stored EPHI, health care organizations may want to consider encrypting EPHI stored on their computer equipment, says Wood. This is especially true for portable equipment, adds Geyer. Laptops, PDAs, portable hard drives, and USB devices can store large amounts of EPHI, and all are good candidates for encryption, she says. That's because they're more likely to be lost, stolen, or used inappropriately. As an example, by encrypting the EPHI stored on these devices, you can greatly reduce the risk that a stranger will be able to access EPHI on a PDA that one of your physicians has left at an airport.

Here's some Model Language that you can use in your security policies if your organization chooses to encrypt information stored on its equipment. We adapted it from Wood's book, *Information Security Policies Made Easy* (ISBN# 1-881585-09-3), available at www.amazon.com.

Model Language
All patient and customer EPHI stored on computer equipment owned or used by the Organization must be encrypted.

***Insider* Says:** There are alternatives to using encryption to prevent access to EPHI on your computer equipment. For instance, many organizations choose to password-protect EPHI stored on computer equipment, instead of encrypting it, says Berkeyheiser. That may be adequate, depending on the circumstances, she adds. For example, if you have a desktop PC that's located in a locked room and has strong password and authentication features, you probably won't need to encrypt the EPHI stored on it.

EPHI stored on backups and archives. EPHI stored on backup media or for archival purposes might not always need to be encrypted. "Encryption is usually appropriate if you're planning on storing EPHI for a long time—say, when you're creating a full backup of your system or an archive disk," notes health care attorney Susan Miller. "But backups that are frequently written over, such as daily backups, might not warrant the recovery problems or extra time it takes to encrypt them," she adds.

"Keep in mind that encryption of backups will often slow, if not prevent, the recovery of the information involved," says Wood. For example, the decryption keys may be unavailable when you urgently need to recover EPHI from backup media. But if you store backup media at commercial storage facilities, the physical access controls usually aren't as good as those at the health care organization's facility. "Backup storage sites are frequently unattended and are accessible by every organization that stores backups there," cautions Wood.

So how do you know whether you should encrypt EPHI stored on backup and archive media? Wood and Geyer suggest that you consider where the data will be stored. If it's stored securely, in a locked location, encryption might not be necessary, especially given the amount of time it will add to the backup and recovery process. But if you have an employee who stores backup tapes at home, that information should be encrypted, Miller advises, because anyone in the home could access it without authorization.

Here's some Model Language, adapted from Wood's *Information Security Policies Made Easy*, that you can include in your security policies if you choose to encrypt EPHI stored off-site on backup and archive media:

Model Language
All patient and customer EPHI recorded on backup or archive computer media and stored outside the Organization's facilities must be encrypted.

(continued on p. 4)

ENCRYPTION: WHAT YOU SHOULD DO
(continued from p. 3)

EPHI transported via couriers. Experts agree that for access control purposes, it's probably not necessary to encrypt EPHI stored on a disk or other form of media that will be transported via couriers—such as the U.S. Postal Service or Federal Express. Simply enclosing the disk or other media in an envelope is usually sufficient. "The probability is very low that someone will attempt to access it," says Berkeyheiser.

But encryption may be appropriate when you want to do more than just control access. Organizations can use digital signatures, an encryption-based procedure, to detect EPHI tampering and alterations. "When computer storage media go through airport X-ray machines and are subjected to other magnetic fields en route, there's a chance that certain parts of the information on them will be erased or altered," explains Wood. If EPHI is digitally signed, erasures and alterations may be highlighted immediately. For that reason, you may want to digitally sign transported EPHI to protect its integrity.

If your organization decides to encrypt and digitally sign EPHI transported via couriers, you can use the following Model Language, adapted from Wood's *Information Security Policies Made Easy*, in your security policies:

Model Language
All patient and customer EPHI transported via computer-readable storage media must be encrypted for confidentiality purposes and digitally signed for authenticity/integrity purposes.

***Insider* Says:** If you decide not to encrypt EPHI—whether at rest or in transit—make sure you document your decision and its rationale. To find out more, see "How to Document Decision Not to Adopt 'Addressable' Implementation Specification," *Insider*, July 2003, p. 1. ■

Insider Sources

Lesley Berkeyheiser: Principal, The Clayton Group, 53 Bethel Rd., Glen Mills, PA 19342; lberkeyheiser@theclaytongroup.org.

Ann Geyer: Partner, Health Care Practice, Tunitas Group, PO Box 278, 6693 Sierra Vista Lookout, Mountain Ranch, CA 95246-0278; ageyer@tunitas.com.

Jim Klein: Vice President and Research Director, Gartner Research, 8405 Greensboro Dr., 6th Fl., McLean, VA 22102; Jim.Klein@gartner.com.

Susan Miller, Esq.: Director of Regulatory Compliance, Optimal Practice Solutions, 276 Harrington Ave., Concord, MA 01742; tmsam@aol.com.

Charles Cresson Wood, CISSP: InfoSecurity Infrastructure, Inc., PO Box 2877, Sausalito, CA 94966-2877; ccwood@ix.netcom.com.

DOS & DON'TS

✓ Attach All PCs to Your Network

If your organization's computer system uses a network drive, make sure you attach each personal computer (PC) that contains electronic protected health information (EPHI) to that network. Stand-alone PCs that aren't attached to your network create huge security problems, says Stephen Wiggin, security analyst for a large insurance company.

Most health care organizations connect all their PCs to a network, says Wiggin. But some organizations—especially if they're small or mid-sized—have one or two PCs with EPHI on them that aren't connected to the network, either because they were overlooked or aren't often used. If your organization allows stand-alone PCs that aren't attached to your network, you'll have to implement controls that limit access to each of those PCs to authorized personnel only. This can be complicated and expensive. Plus you'll need to back up your information on each stand-alone PC as often as you back up your organization's network drive, which can be time consuming. And you could have difficulty finding EPHI on a stand-alone PC that isn't attached to the network.

"But if you attach each PC to your network, access control issues can be easily addressed, and nightly backups can be performed right from the network drive," says Wiggin. Another advantage is that all of your information will be in one place. So if you need to access someone's EPHI for legal reasons—such as to respond to a subpoena—you won't have to check each PC to see what's on it, he adds.

✗ Don't Overlook Addressable Implementation Specifications During Security Analysis

When performing your security analysis—that is, looking at what your organization needs to do to comply with the HIPAA security regulations—don't forget to include addressable implementation specifications on your list, says health information technology expert Sybil Ingram-Muhammad. Otherwise, your security analysis will be

incomplete and you'll be in violation of the HIPAA security regulations.

Many of the standards in HIPAA's security regulations include both required and addressable implementation specifications. You may think that you must consider only the required implementation specifications when performing your security analysis. But the security regulations say that you must look at the addressable implementation specifications, too, says Ingram-Muhammad. "Just because an implementation specification is addressable doesn't mean you can avoid it altogether," she warns. "You're going to have to review an addressable specification, just like you would a required specification," she explains.

The difference is that with an addressable implementation specification—as opposed to a required implementation specification—you can choose not to implement it if it's not reasonable and appropriate to your organization. "However, if you choose not to implement it, you must document the reason why and explain any alternatives you may have chosen to meet the standard," Ingram-Muhammad adds. ■

Further reading: Insider, July 2003, p. 1: "How to Document Decision Not to Adopt 'Addressable' Implementation Specification."

Insider Sources

Sybil Ingram-Muhammad, MBA, PhD: Senior Practice Director, Healthcare Privacy and Security Solutions Practice, IntelliMark I.T. Business Solutions, 5295 Hwy. 78, Ste. D, #288, Stone Mountain, GA 30087; smuhammad@Intellimark-IT.com.

Stephen Wiggin, CISSP: Sr. Security Analyst, Mutual of Omaha, Mutual of Omaha Plz., Omaha, NE 68175; Steve.wiggin@mutualofomaha.com.

ASK THE *INSIDER*

The INSIDER *welcomes questions from subscribers. You can 1) send your questions to* HIPAA Security Compliance Insider, *Brownstone Publishers, Inc., 149 Fifth Ave., 16th Fl., New York, NY 10010-6801; 2) call (908) 757-2843, and speak with the editor; 3) fax (908) 757-2844; or 4) e-mail awatkins@brownstone.com*

Using Taxonomy Codes

Q Payors keep rejecting our electronic claims because of missing or invalid taxonomy codes. Do HIPAA's transaction and code sets (TCS) standards require us to use taxonomy codes? Where can we get the most recent codes to make sure our claims aren't rejected?

A Although the taxonomy codes are one of the code sets named in many of the X12N implementation guides adopted for use under HIPAA's TCS standards, their use is situational, says HIPAA transactions consultant Margret Amatayakul. This means the codes are required when the situation calls for them, she explains. So if a payor determines that a taxonomy code is necessary to process a claim, it can require a provider to include the proper taxonomy code on its claim form. Many payors require providers to include taxonomy codes on all electronic claim forms.

Here's some background on taxonomy codes, and details on where to find them and how to determine if your payor requires them:

What are taxonomy codes? Taxonomy codes are 10-digit numbers maintained by the National Uniform Billing Committee. Health care providers use taxonomy codes to inform payors of the provider's specialty and subspecialty. For example, just for optometrists, there are six different taxonomy codes:

- Corneal and Contact Management (Code: 152WC0802X);
- Low Vision Rehabilitation (Code: 152WL0500X);
- Occupational Vision (Code: 152WX0102X);
- Pediatrics (Code: 152WP0200X);
- Sports Vision (Code: 152WS0006X); and
- Vision Therapy (Code: 152WV0400X).

If a payor requires a provider to use taxonomy codes when submitting claim forms, the provider probably won't use the same taxonomy code for every claim. For example, an optometrist treating a child would use the taxonomy code for Optometrist: Pediatrics. But if the same optometrist treated an adult, he would use a different taxonomy code.

Where are the codes listed? If a payor requires that you use taxonomy codes on your electronic claim forms, your claims will be rejected unless you use a valid code, warns Amatayakul. You can find a list of approved taxonomy codes at the Washington Publishing Company Web site at www.wpc-edi.com/codes/codes.asp. Click on the pull-

(continued on p. 6)

ASK THE *INSIDER* (continued from p. 5)

down menu under "Code Lists" and select "Provider Taxonomy Codes."

The codes are updated every April and October. And because they're nonmedical codes, you must use the codes in effect at the time you submit the claim—rather than the codes in effect at the time of treatment, which might be different.

Where are the payor requirements set out? To find out if and when your payors require you to use taxonomy codes, Amatayakul recommends that you check each payor's companion guide, which clarifies that payor's transactional requirements. If a payor doesn't have a companion guide or you're uncertain about whether to include taxonomy codes in your transactions, err on the side of inclusion, she says. Otherwise, your transactions might be rejected. ■

Further reading: Insider, Oct. 2003, p. 5, "TCS: Use Valid Codes for Electronic Transactions."

Insider Source

Margret Amatayakul, RHIA, CHPS, FHIMSS: President, Margret\A Consulting, LLC, 2313 W. Weathersfield Way, Schaumburg, IL 60193; margretcpr@aol.com.

Make Sure Data Backup Plan Covers EPHI Stored in Handheld Devices

by Daniel P. Dern

Daniel P. Dern *(ddern@world.std.com) is a freelance technology writer. Most recently he was executive editor of Byte.com. His Web site is www.dern.com.*

The HIPAA security regulations require health care organizations to establish and implement procedures for retrieving exact copies of electronic protected health information (EPHI). To meet this requirement, you must deal with a tricky problem: backing up EPHI stored in personal digital assistants (PDAs) and other handheld devices (for example, the Palm Pilot, Blackberry, and Hewlett Packard iPAQ models). This is tricky because most of these devices store data in "volatile" memory (also called "RAM"). With volatile memory, if the device's battery loses power, stored data, including EPHI disappears. And since most handheld devices run on batteries rather than wall current, loss of power is common.

To comply with the HIPAA security regulations, you must create a policy setting out appropriate procedures for staff with handhelds to use to guard against letting the power run out on the handhelds; you also must have them properly back up EPHI stored in volatile memory—that is, save it to an external location with non-volatile memory so it's available if power does run out (or the device is damaged, lost, or stolen). Here's how to create such a policy. There's also a Model Policy (see p. 7) that you can adapt.

How to Write a Policy

Like our Model Policy, your policy should do three things:

Warn users of possible data loss. Start your policy by warning users that if their handheld loses power, they'll lose stored data, including EPHI. Don't assume users realize this. Although handhelds typically include a warning to this effect in the users manual, many users don't notice the warning, says mobile device expert Chris De Herrera. "The loss of stored data to a dead battery is so common that most users experience it at least once before learning that they need to keep their device constantly charged," De Herrera adds. So explain the risk again. And set off your warning in boldface type [Pol., par. 1].

Tell users to keep batteries charged. Next tell users to keep their handheld batteries constantly charged. Clear up the common misconception that all users need to do to preserve the battery is turn off the POWER button. "That just shuts down the display and powers down the processor," explains handhelds expert John Ruley. "The battery will continue to provide power to the memory. So a battery can still run out when a device has been 'turned off,' " he notes. And put this information in boldface so it's tough for users to overlook. Then tell users to:

- Perform regular battery checks following the procedures set out in the users manual [Pol., par. 2(a)].
- Change batteries immediately if they get a "Low-Battery" signal, and keep extra batteries on hand, including "bridge" batteries. "Some handhelds include an extra 'bridge' battery that supplies a few minutes of power to the memory if the primary battery dies," explains De Herrera. That's enough to

(continued on p. 8)

MODEL POLICY

Alert Users of PDAs and Other Handhelds to Data Loss Risk and Prevention Methods

The HIPAA security regulations require health care organizations to have a data backup plan to protect electronic protected health information (EPHI), including EPHI stored in PDAs and other handheld devices that use volatile memory. Such data is especially vulnerable because if the device loses power, all stored data is wiped out. One step in complying with this requirement is to create a policy to get personnel who use PDAs and other handhelds to keep their batteries charged and to back up EPHI to non-volatile locations just in case the power goes off.

Here's a Model Policy to ensure that PDA and handheld users take the proper precautions. It was prepared with the help of California attorney Stephen M. Fleisher and Massachusetts consultant Robert P. Laramie. Adapt it to your own circumstances, and add it to your overall information security policy.

BACKUP OF DATA STORED ON PDAS & HANDHELDS

1. **WARNING TO PDA/HANDHELDS USERS.** Unlike desktop and notebook PCs, which store data on hard disks, most personal digital assistants (PDAs) and other handheld devices store data in "volatile" memory. **If you use a PDA and/or handheld, be aware that any data you store on the device may be irretrievably lost if the battery that powers the device runs out.** Such data includes not only contact and calendar information but also electronic protected health information (EPHI) covered by HIPAA. The purpose of this policy is to ensure compliance with HIPAA by setting forth measures for users to take to back up EPHI and other data stored on PDAs and handhelds.
2. **KEEP BATTERIES CHARGED.** Do not let the battery running your PDA or handheld run out. **Simply turning off the POWER button on your device is not enough. The battery continues to function and thus can still drain when the POWER button is toggled to "off."** To save the battery you must take the following steps:
   a. Regularly check the device's battery level in accordance with the instructions in the users manual.
   b. If your device has a replaceable battery, change it immediately if you see a "Low Battery" signal. Keep extra batteries, including primary and bridge batteries if your device uses both.
   c. If your PDA or handheld device has a rechargeable battery, regularly recharge the battery in accordance with the user manual's instructions. We suggest recharging the battery every day. In no event should you allow the battery level to fall below 40 percent. Buy a charger and any other accessory necessary to recharge the battery. If you intend to travel with your PDA or handheld, consider buying an extra charger that you can take with you while you're away.
   d. If you know you won't be using the PDA or handheld device for a prolonged period, leave it in a secure place plugged into a source that will keep the batteries charged while the device is not in use.
3. **REGULAR BACKUPS.** Regularly back up EPHI and other data you store on your PDA or handheld so that you'll always be able to retrieve an exact copy in case your PDA or handheld device runs out of power (or is damaged, lost, or stolen), using any one or more of the following procedures, as may be called for by your device's users manual:
   a. Ensure the constant synchronization of EPHI in real time using wireless connections or other methods and devices in accordance with the PDA or handheld's users manual.
   b. Regularly—that is, at least once a day on any day you create or change EPHI—save EPHI and any other data you enter into your PDA or handheld following the instructions set out in the PDA or handheld device's users manual and/or external backup programs you've installed on the device. If the instructions call for it, use a wireless connection or otherwise ensure the constant synchronization of EPHI in real time. Before storing actual data on the device, create a "dummy" sample and try backing it up so you can test the procedure to confirm that you understand it and that it actually works.
   c. Make sure synchronized or saved data is stored on a hard disk in a computer such as your notebook/desktop computer and/or a server run by XYZ Clinic.
   d. As an additional precaution, download data from your PDA or handheld device to a floppy disk, writeable CD, external hard drive, ZIP drive, CF or SmartMedia card, etc., and store it in a secure location like a locked file drawer.
   e. Determine and obtain whatever equipment (e.g., a charging/synching cradle and HotSync cable), media (e.g., backup software), and/or connections (e.g., between your PDA or handheld and your notebook/desktop computer) you'll need to perform the necessary backup procedures.

DATA BACKUP PLAN (continued from p. 6)

preserve the memory while the battery is changed [Pol., par. 2(b)].

■ Regularly recharge the battery. "Users should recharge the battery every day and not wait for a battery low signal," notes De Herrera. We also caution users against letting their battery level fall below 40 percent [Pol., par. 2(c)].

■ Leave the device charging when it's not in use for a prolonged period [Pol., par. 2(d)].

Tell users to back up data. Users should also back up data to another source in case their handheld device loses power (or gets damaged, lost, or stolen). So tell users to:

■ Use wireless connections or otherwise ensure the constant synchronization, or "synching," of EPHI and other data in real time. Synching ensures that data are up-to-date on both the device and a "host" (the connected notebook, desktop computer, or server). Providing for real-time constant synchronization enables physicians and other medical personnel to concentrate on treating patients in emergencies without distraction [Pol., par. 3(a)]; and/or

■ Save EPHI and any other data they enter into their handheld on a regular basis—that is, at least once on any day when they create or modify EPHI.

The backup procedures vary depending on the devices and applications involved. So our policy simply tells users to follow the instructions in the handheld's users manual and/or external backup programs they've installed on the device. It also tells users to test the backup procedure to make sure they understand it and confirm that it works [Pol., par. 3(b)].

***Insider* Says:** Tell users to contact your organization's IT personnel if the test doesn't work. They'll need to use a separate backup program like Blue Nomad's BackupBuddy for Palm OS devices or BSquare's bUSEFUL Backup Plus for Pocket PCs and Windows CE devices.

■ Regardless of the backup procedure used, make sure that saved data gets stored to a hard disk on a computer (such as a desktop or notebook computer) or, depending on your IT environment, directly to a server run by your organization. This means that a copy will be available in case the handheld runs out of power (or gets damaged, lost, or stolen) [Pol., sec. 3(c)].

■ As an extra precaution, regularly download the data to another nonvolatile memory source, such as a floppy disk, writeable CD, external hard drive, ZIP drive, CF or SmartMedia card, and store this extra copy in a secure location like a locked file drawer [Pol., par. 3(d)].

■ Get whatever equipment, media, or connections are necessary to perform the backup procedure. For example, the user may need a connection between the handheld and a host; special equipment like a charging cradle or synching cable; and a backup program or other software, applications, and utilities [Pol., par. 3(e)]. ■

Insider Sources

Chris De Herrera: Creator, CEWindows.NET; webmaster@cewindows.net.

Stephen M. Fleisher, Esq.: Fleisher & Assocs., 35 Corwin Dr., Alamo, CA 94507.

Robert P. Laramie: President, New Tech Consultancy, Inc., 800 Turnpike St., Ste. 300, North Andover, MA 01845; rlaramie@newtechconsultancy.com.

John Ruley: Contributing Editor, Windows & .NET Magazine; jruley@ainet.com.